UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,505	03/30/2004	Stephen R. Carter	1565.073US1	4898

21186 7590 04/01/2008

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
04/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,505	CARTER, STEPHEN R.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2004* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see attached PTO form 1449's*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statements (IDS) submitted are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Asano, U.S. Patent 7,088,822.

As per claim 1, it is taught by Asano of a method for dynamically managing security associated with document collaboration, comprising associating collaborators with different encrypted versions of a key, wherein decrypted versions of the key permit access to a document; and adding an identity service as one of the collaborators, wherein the identity service is capable of dynamically adjusting encryption formats for

one or more of the collaborators' encrypted keys (col. 21, lines 25-67 and col. 22, line 48 through col. 23, line 10).

As per claim 2, Asano discloses of dynamically adding or removing one or more of the collaborators (col. 20, line 43 through col. 21, line 9).

As per claim 3, Asano teaches of linking the collaborators and encrypted keys to the document as metadata defining document access and security (col. 4, lines 32-43 and col. 35, lines 35-48).

As per claim 4, it is disclosed by Asano of embedding the collaborators and encrypted keys within a portion of the document defining document access and security (col. 4, lines 32-43 and col. 35, lines 35-48).

As per claim 5, it is taught by Asano wherein adding further includes recognizing a select one of the collaborators as trusted to the identity service and permitting it to provide a dynamically generated public key which the identity service uses to encrypt a select one of the encrypted keys associated with the trusted collaborator (col. 4, lines 32-43; col. 21, lines 25-67; and col. 22, line 48 through col. 23, line 10).

As per claim 6, it is disclosed by Asano wherein adding further includes inspecting a community list associated with the document to determine if the select one of the collaborators is authorized to be the trusted (col. 4, lines 32-43).

As per claim 7, Asano teaches wherein signing the document by a select one of the collaborators which modifies the document, wherein the signature is associated with a public key of the select collaborator (col. 4, lines 32-43).

As per claim 8, Asano discloses of changing the key; and updating the encrypted versions of the key with the changed key (col. 20, line 43 through col. 21, line 9).

As per claim 9, it is taught by Asano of a method for dynamically managing security associated with document collaboration, comprising identifying a collaborator associated with a document; verifying a trust relationship between the collaborator and the document; acquiring a dynamic public key from or on behalf of the collaborator; decrypting a symmetric key which grants access to the document; and encrypting the symmetric key with the dynamic public key (col. 4, lines 32-43; col. 12, lines 54-61; col. 21, lines 25-67; and col. 22, line 48 through col. 23, line 10).

As per claim 10, it is disclosed by Asano of recognizing that the collaborator has altered the document and signed the document with the dynamic public key; and communicating the dynamic public key to a plurality of other collaborators associated with the document (col. 4, lines 32-43).

As per claim 11, Asano teaches wherein acquiring further includes acting as an intermediary between the collaborator and key service for purposes of acquiring a strongly rooted key pair for the collaborator, wherein a portion of that key pair is the public key and wherein another portion of that key pair is a private key which permits the collaborator to decrypt the encrypted symmetric key for purposes of accessing the document (col. 4, lines 32-43; col. 12, lines 54-61; col. 21, lines 25-67; and col. 22, line 48 through col. 23, line 10).

As per claim 12, Asano discloses wherein acquiring further includes generating a non-strongly rooted private-public key pair for the collaborator (col. 4, lines 32-43 col. 4, lines 32-43).

As per claim 13, it is taught by Asano of dynamically receiving a request from a different collaborator to access the document; inspecting a trust specification to ensure the access is permissible; receiving a public key for the different collaborator; generating a new symmetric key which includes the different collaborator, the collaborator, and other collaborators associated with the document; and encrypting the symmetric key with the public key of the different collaborator and with the dynamic public key of the collaborator and with other public keys associated with the other collaborators (col. 4, lines 32-43; col. 12, lines 54-61; col. 21, lines 25-67; and col. 22, line 48 through col. 23, line 10).

As per claim 14, it is disclosed by Asano of further comprising, communicating the public key of the different collaborator to the collaborator and to the other collaborators associated with the document (col. 4, lines 32-43).

As per claim 15, Asano teaches wherein generating further includes generating a random new symmetric key (col. 12, lines 54-61).

As per claim 16, Asano discloses wherein inspecting further includes inspecting community lists associated with the different collaborator and the document to ensure that the different collaborator can be dynamically added as a new collaborator to the document (col. 20, line 43 through col. 21, line 9).

As per claim 17, it is taught by Asano wherein verifying further includes authenticating the collaborator to the document according to a contract (col. 4, lines 32-43).

As per claim 18, it is disclosed by Asano of a dynamic collaborative document security system, comprising a document; a list of collaborators associated with the document; and an identity service, wherein the identity service is included within the list of collaborators, and wherein the identity service dynamically manages encryption of a symmetric key associated with the document and dynamically manages identities of the list of collaborators according to a trust specification, wherein access to a decrypted version of the symmetric key provides access to the document (col. 4, lines 32-43; col. 12, lines 54-61; col. 21, lines 25-67; and col. 22, line 48 through col. 23, line 10).

As per claim 19, Asano teaches wherein each entry within the list of collaborators includes a specific encrypted version of the symmetric key, each specific encrypted version is encrypted with a specific public key of a specific collaborator included within the list of collaborators (col. 4, lines 32-43; col. 12, lines 54-61 and col. 21, lines 25-67).

As per claim 20, Asano discloses wherein the identity service changes the symmetric key and re-performs encryption when a specific collaborator is dynamically added to or dynamically removed from the list of collaborators (col. 20, line 43 through col. 21, line 9).

As per claim 21, it is taught by Asano wherein the identity service dynamically acquires a strongly rooted public-private key pair on behalf of a requesting collaborator from a keying service (col. 4, lines 32-43).

As per claim 22, it is disclosed by Asano wherein the identity service dynamically generates a non-strongly rooted public-private key pair on behalf of a requesting collaborator (col. 4, lines 32-43).

As per claim 23, Asano teaches wherein the identity service determines if a dynamically generated public key associated with a specific collaborator of the list of collaborators has signed the document after altering the document, and wherein if this occurs the identity service communicates the dynamically generated public key to the remaining collaborators included within the list of collaborators (col. 4, lines 32-43 and col. 22, line 48 through col. 23, line 10).

As per claim 24, Asano discloses of further comprising access control rights associated with each collaborator included within the list of collaborators (col. 35, lines 35-48).

As per claim 25, it is taught by Asano of a document residing in a computer readable medium, comprising content data; a symmetric key; and a list of collaborators, each collaborator within the list associated with a specific encrypted version of the symmetric key, wherein an identity service is included within the list of collaborators, the identity service capable of dynamically adding and removing select ones of the collaborators and capable of dynamically re-encrypting the symmetric key for the select ones of the collaborators (col. 4, lines 32-43; col. 12, lines 54-61; col. 21, lines 25-67; and col. 22, line 48 through col. 23, line 10).

As per claim 26, it is disclosed by Asano wherein the document is at least one of an executable program, a directory, a resource, a file, an image, and a video (col. 2, lines 14-16).

As per claim 27, Asano teaches wherein the symmetric key and the list of collaborators are metadata linked with the content data (col. 12, lines 54-61 and col. 35, lines 35-48).

As per claim 28, it is disclosed by Asano of further comprising a trust specification that defines relationships between collaborators and the document, and wherein the trust specification drives the actions of the identity service (col. 4, lines 32-43 and col. 35, lines 35-48).

As per claim 29, it is taught by Asano of further comprising a community list which is consumed by the identity service, the community list identifying collaborators which can be dynamically added to the list of collaborators (col. 20, line 43 through col. 21, line 9).

As per claim 30, Asano discloses wherein members of the list of collaborators have been granted access control rights or edit rights to the document via the identity service which determines the access control rights or edit rights based on a trust specification for the document (col. 4, lines 32-43 and col. 35, lines 35-48).

As per claim 31, Asano teaches wherein the identity service communicates a trust specification of the document dynamically to another service, and wherein that service uses the trust specification to dynamically manage access to the document (col. 4, lines 32-43 and col. 35, lines 35-48).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/
Primary Examiner, Art Unit 21311